UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/688,499	10/17/2003	Kumar Ranganathan	42P17239	1968

8791 7590 04/06/2007

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
CALLAHAN, PAUL E	
ART UNIT	**PAPER NUMBER**
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/688,499	RANGANATHAN, KUMAR	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *9-16,28 and 29* is/are allowed.

6)☒ Claim(s) *1-5 and 17-26* is/are rejected.

7)☐ Claim(s) *6-8, 27,and 30* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10-16-03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 are pending in the instant application and have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-5, 17, 18, 20-22, 24-26 are rejected under 35 U.S.C. 102(b) as being clearly anticipated by Arbaugh et al., "A Secure and Reliable Bootstrap Architecture" IEEE 1997, pp. 65-71.

As for claim 1, Arbaugh teaches a method, comprising: generating a first level trusted computing base (TCB) having a plurality of hardware components including a trusted platform module (TPM) (Sec. 3.1 Overview: PROM board containing verification code and public key certificates, Sec. 3.2.2 AGEIS BIOS Modifications: a verification checksum is calculated, this constitutes the implementation of a TPM); forming an extended TCB by adding a second level TCB to the first level TCB (Sec. 3.2: AGES Boot Process: BIOS checks for expansion card ROM signature, Sec. 3.2.2: upon verification ROM executes and control is ultimately passed to the operating system

bootstrap code), wherein the second level TCB is software-based; and transferring properties associated with the first level TCB to the second level TCB (Sec. 3.2.2)

As for claim 2, Arbaugh teaches the method of claim 1, wherein the transferring of the properties is performed using a first level TCB interface having at least one of the following operations: secure storage, initiation of software integrity measurement, and attestation (Sec. 3.1 Overview: PROM board containing verification code and public key certificates, Sec. 3.2: AGES Boot Process: BIOS checks for expansion card ROM signature).

As for claim 3, Arbaugh teaches the method of claim 1, wherein the properties associated with the first level TCB comprise trust and security properties including at least one of the following: tamper-resistant secure storage, tamper-resistant software measurement, tamper-resistant attestation of previously measured values via tamper-resistant signature algorithms, and private keys (Sec. 3.1 Overview: PROM board containing verification code and public key certificates: by definition, public key certificates will have a signed hash of the public key, i.e., signed with the corresponding private key).

As for claim 4, Arbaugh teaches the method of claim 1, further comprising: adding one or more levels of software-based TCB to the extended TCB (Figure 3: BIOS Section 2, Boot Block, Sec. 3.2.2: Control is passed to the Boot Block), and transferring

the properties associated with the first level TCB to the one or more levels of software-based TCB via one or more levels of TCB interfaces (Sec. 3.2.2: Control is passed to the Boot Block).

As for claim 5, Arbaugh teaches the method of claim 4, wherein a level of software-based TCB of the one or more levels of software-based TCB of a first system intact with a counterpart level of software TCB of a second system independent of other levels of the one or more levels of software-based TCB of the first system (Sec. 3.2.2: integrity check failures are recovered by a call to a network host in one embodiment, a TCB on a network server is inherent).

As for claims 17, 18, 20-22, 24-26, the claims are directed towards the apparatus that carries out the method of claims 1-5. Claims 17, 18, 20-22, and 24-26 recite substantially the same limitations as claims 1-5 and are therefore rejected on the same basis as those claims.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 19 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arbaugh.

Arbaugh does not explicitly teach a step wherein the plurality of hardware components comprises a chipset to couple the TPM with the processor. However Official Notice may be taken that the use of a chipset to couple a TPM with a processor is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Arbaugh. It would have been desirable to do so since this would allow for the use of industry standard chipsets in implementation of the TPM on a computing device, hence increasing the utility of the system.

Allowable Subject Matter

6. Claims 9-16, 28, and 29 are allowed.

7. Claims 6, 7, 8, 27, and 30, are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

8. The following is a statement of reasons for the indication of allowable subject matter: The closest prior art in the field fails to teach the combination of features found in the claims, particularly including:

As for claim 6, using one or more levels of software TCB independent of hardware-based or software-based implementation of a level of software TCB below the one or more levels of software TCB.

As for claims 7 and 8, a second level TCB that is executed independent of a first level TCB using a processor and main memory of a system.

As for claim 27, the feature where the second level TCB and the one or more levels of software-based TCB use encryption keys for attestation and secure storage, the encryption keys are encrypted using protected encryption keys in a TCB level below the second level TCB. Claim 30 is dependent from claim 27 and is objected to on that basis.

As for claims 9 and 28, the feature where of adding a first virtual software TPM to the second level TCB; and transferring properties associated with a hardware TPM of the first level TCB to the first virtual software TPM. Claims 10-16 and 29 are dependent on claims 9 and 28 respectively and are allowable on that basis.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following US Patent documents teach systems of Trusted Computing Base configuration and expansion pertinent to the applicant's disclosure:

Arbaugh et al.	6,185,678
Focke et al.	7,103,914
Zimmer et al.	6,978,018
Zimmer et al.	7,127,579

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PEC
3-30-07

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER